

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月30日

出 願 番 号

Application Number:

特願2002-287116

[ST.10/C]:

[JP2002-287116]

出 願 人

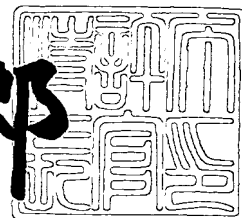
Applicant(s):

株式会社東芝

2003年 1月24日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3001300



【書類名】 特許願

【整理番号】 A000204058

【提出日】 平成14年 9月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明の名称】 ネットワーク中継装置、通信装置、及びネットワーク中継方法

【請求項の数】 13

【発明者】

 【住所又は居所】 東京都青梅市末広町2丁目9番地 株式会社東芝青梅事業所内

 【氏名】 小久保 隆

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

 【弁理士】

 【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク中継装置、通信装置、及びネットワーク中継方法

【特許請求の範囲】

【請求項 1】 複数のネットワークを中継するべく通信を行うネットワーク中継装置であり、

第1ネットワークに接続され、鍵情報により暗号化されたコンテンツ情報を送受信する第1インタフェースと、

前記第1ネットワークとは異なる第2ネットワークに接続され、前記コンテンツ情報を中継相手のネットワーク中継装置に対し送受信する第2インタフェースと、

前記第1インタフェースからの前記コンテンツ情報を暗号化した前記鍵情報が変更されたかどうかを前記第1インタフェースを介して検出し、前記鍵情報に変更があるとき鍵変更通知信号を前記第2インタフェースを介して受信側のネットワーク中継装置の前記第2インタフェースに通知する通知部と、

を具備することを特徴とするネットワーク中継装置。

【請求項 2】

送信側のネットワーク中継装置の前記通知部から前記第2インタフェースを介して前記鍵変更通知信号を受けた時、前記第2ネットワークから受けた前記コンテンツ情報の前記第1ネットワークへの送信を所定時間中断した上で再開するべく制御する制御部を有することを特徴とする請求項1記載のネットワーク中継装置。

【請求項 3】

送信側のネットワーク中継装置からの前記コンテンツ情報の送信が中断した時、前記通知部から前記第2インタフェースを介して前記鍵変更通知信号を受けない場合は前記コンテンツ情報の代わりに空データを前記第1インタフェースを介して通信装置に送信し、前記鍵変更通知信号を受けた場合は前記コンテンツ情報の前記通信装置への送信を一時中断するべく制御する制御部を有することを特徴とする請求項1記載のネットワーク中継装置。

【請求項 4】

送信側のネットワーク中継装置の前記通知部から前記第 2 インタフェースを介して前記鍵変更通知信号を受けた時、これを前記第 1 インタフェースを介して前記第 1 ネットワークに接続される通信装置へ送信するべく制御する制御部を有することを特徴とする請求項 1 記載のネットワーク中継装置。

【請求項 5】

前記第 1 インタフェース及び前記第 2 インタフェースは、D T C P (Digital Transmission Content Protection) 規格により前記鍵情報を用いて暗号化された前記コンテンツ情報を送受信することを特徴とする請求項 1 記載のネットワーク中継装置。

【請求項 6】

前記通知部は、D T C P 規格による前記鍵情報を問い合わせるコマンドを用いて前記鍵情報を取得し、取得した鍵情報と以前の鍵情報とを比較して、鍵情報が変更されたかどうかを判断することを特徴とする請求項 1 記載のネットワーク中継装置。

【請求項 7】

ネットワークに接続されるインタフェースを介し、前記ネットワークに接続されるネットワーク中継装置を経由して他のネットワーク上の通信装置と、鍵情報により暗号化されたコンテンツ情報の通信処理を行う通信部と、

前記通信部が前記インタフェースを介して、ネットワーク中継装置から鍵変更通知信号を受けた時、前記他のネットワーク上の前記通信装置へ、新たな鍵情報を取得するための信号を送信して新しい鍵情報を受け、この新しい鍵情報に基づき前記コンテンツ情報を復号化して出力する制御部と、

を具備することを特徴とする通信装置。

【請求項 8】 複数のネットワークを中継するべく通信を行うネットワーク中継方法であり、

第 1 ネットワークに接続され、鍵情報により暗号化されたコンテンツ情報を送受信する第 1 インタフェースと、前記第 1 ネットワークとは異なる第 2 ネットワークに接続され、前記コンテンツ情報を中継相手のネットワーク中継装置へと送受

信する第 2 インタフェースとを有するネットワーク中継装置を用いて、

前記第 1 インタフェースからの前記コンテンツ情報を暗号化した前記鍵情報が変更されたかどうかを前記第 1 インタフェースを介して問い合わせ、

この問合せの回答信号を受け、前記鍵情報に変更があるとき鍵変更通知信号を前記第 2 インタフェースを介して前記中継相手のネットワーク中継装置の前記第 2 インタフェースに通知する、

ことを特徴とするネットワーク中継方法。

【請求項 9】

送信側のネットワーク中継装置の前記通知部から前記第 2 インタフェースを介して前記鍵変更通知信号を受けた時、前記第 2 ネットワークから受けた前記コンテンツ情報の前記第 1 ネットワークへの送信を所定時間中断した上で再開するべく制御することを特徴とする請求項 8 記載のネットワーク中継方法。

【請求項 10】

送信側のネットワーク中継装置の前記第 2 インタフェースを介して前記鍵変更通知信号を受けた時、これを前記第 1 インタフェースを介して前記第 1 ネットワークに接続される通信装置へ送信することを特徴とする請求項 8 記載のネットワーク中継方法。

【請求項 11】

送信側のネットワーク中継装置からの前記コンテンツ情報の送信が中断した時、前記第 2 インタフェースを介して前記鍵変更通知信号を受けない場合は前記コンテンツ情報の代わりに空データを前記第 1 インタフェースを介して通信装置に送信し、前記鍵変更通知信号を受けた場合は前記コンテンツ情報の前記通信装置への送信を一時中断するべく制御することを特徴とする請求項 8 記載のネットワーク中継方法。

【請求項 12】

前記第 1 インタフェース及び前記第 2 インタフェースは、D T C P 規格により前記鍵情報を用いて暗号化された前記コンテンツ情報を送受信することを特徴とする請求項 8 記載のネットワーク中継方法。

【請求項 13】

前記鍵変更通知信号は、D T C P 規格による前記鍵情報を問い合わせるコマンドを用いて前記鍵情報を取得し、取得した鍵情報と以前の鍵情報とを比較して、鍵情報が変更されたかどうかを判断することにより生成されることを特徴とする請求項 8 記載のネットワーク中継方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、ネットワーク中継装置に関し、特に D T C P (Digital Transmission Content Protection) 規格により暗号化されたコンテンツ情報を扱うネットワーク中継装置、通信装置、及びネットワーク中継方法に関する。

【0 0 0 2】

【従来の技術】

最近、デジタル機器の開発・普及に伴い、これらのネットワーク通信装置についても要請が高まってきている。ネットワーク通信装置においては、デジタル伝送を用いた高速で多機能なデータ伝送が行われている。

例えば、デジタル伝送においては、伝送上に流れるデータ（コンテンツ）の改ざん、複製が容易なため、コンテンツに対する保護技術が必要となる。そのために規格化された技術の一つに、D T C P 規格がある（<http://www.dtcp.com>参照）。この技術は、I E E E 1 3 9 4 高速シリアルバス上を流れるデジタル同期型パケットデータを改ざんや違法な複製から保護するために開発されたものである。その仕様は上記 U R L にて公開されており、デジタルテレビやデジタル V H S との間でデータをやり取りする際にも使用されている。

【0 0 0 3】

この D T C P 規格は、I E E E 1 3 9 4 高速シリアルバスだけにとどまらず、U S B (Universal Serial Bus) などの別のバス規格上で伝送する場合や、異なるネットワークをまたがって伝送する場合などの規格へと拡張されようとしている。

【0 0 0 4】

このような D T C P 規格を用いた従来技術（例えば、特許文献 1 参照）におい

ては、ネットワーク通信装置及びネットワーク中継装置に D T C P 規格に基づく暗号化・復号化処理が行われ、第三者に対するセキュリティを保持した状態でのネットワーク通信が行われている。しかしながらこの従来技術では、暗号化に使用した鍵情報を調べる処理を行ってはいない。

ここで、D T C P 規格において、送信側通信装置はコンテンツの送信を停止した後、再開した場合、再開前の暗号鍵と異なる暗号鍵で暗号化してコンテンツを送る可能性がある。受信側通信装置はコンテンツ伝送の停止を検知できるが、厳密に正確な判定はできないので、送信が停止するたびに、鍵の番号（コンテンツを送信する毎に変わる鍵の番号）を A K E コマンドで確認する必要がある。

従って、送信側の通信装置からの D T C P 規格において暗号化されたコンテンツが停止すると、ネットワーク中継装置においても、受信側の通信装置へ送るコンテンツを停止することとなる。これにより、鍵番号が変わった場合のみならず、単にノイズ等で送信が遅れた場合であっても、受信側の通信装置は、鍵番号を A K E コマンドで確認するため、送受信処理が遅延するという問題がある。

【 0 0 0 5 】

【特許文献 1】

特開 2 0 0 2 - 1 1 1 7 0 3 号公報（第 5 - 6 頁、図 1）。

【 0 0 0 6 】

【発明が解決しようとする課題】

すなわち、従来のネットワーク中継装置においては、D T C P 規格等の暗号化コンテンツを通信する場合、送信側からのコンテンツの遅滞があると、鍵が変わった可能性があるため、ネットワーク中継装置において、受信側の相手のネットワーク中継装置へのコンテンツの送信も一時中断して、受信側の通信装置に A K E コマンドによる鍵番号確認を促す必要がある。しかし、必ずしも鍵が変わった訳ではなく、単にノイズ等でコンテンツ情報が遅延している場合もあり、結果的に受信側通信装置の不要な鍵番号確認が繰り返されることとなり、これが通信遅滞の原因となるという問題がある。

本発明は、鍵情報の変更を検出して鍵情報の変更がある時のみ、コンテンツの送信を一時中断して受信側通信装置に鍵情報確認を促すことにより、通信速度を

向上させたネットワーク中継装置と通信装置及びネットワーク中継方法を提供することを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】

本発明に係るネットワーク中継装置は、上記課題を解決するべく、複数のネットワークを中継するべく通信を行うネットワーク中継装置であり、第1ネットワークに接続され、鍵情報により暗号化されたコンテンツ情報を送受信する第1インタフェースと、前記第1ネットワークとは異なる第2ネットワークに接続され、前記コンテンツ情報を中継相手のネットワーク中継装置へと送受信する第2インタフェースと、前記第1インタフェースからの前記コンテンツ情報を暗号化した前記鍵情報に変更されたかどうかを前記第1インタフェースを介して検出し、前記鍵情報に変更があるとき鍵変更通知信号を前記第2インタフェースを介して受信側のネットワーク中継装置の前記第2インタフェースに通知する通知部とを具備することを特徴とするネットワーク中継装置である。

【 0 0 0 8 】

本発明に係るネットワーク中継装置は、上述したように、送信側通信装置からのコンテンツ情報の鍵情報の変更があるかどうかを検出し、変更がある場合に、鍵変更通知信号を受信側のネットワーク中継装置に送信するものである。こうすることにより、受信側のネットワーク中継装置では、鍵情報の変更を知ることができる。これにより、従来のネットワーク中継装置のように、複数のネットワーク上の通信装置同士の中継処理を行う際に、送信側通信装置からのコンテンツ情報の受信が中断すると、ネットワーク中継装置においても、受信側通信装置へのコンテンツ情報の送信を中断する必要がなくなる。すなわち、コンテンツ情報の受信が中断しても、鍵情報の変更がないときはコンテンツ情報の代わりに空データ（空パケット）をネットワーク上の受信側通信装置に送信することで、無駄に鍵情報の取得コマンドを送信して、通信が遅延することを回避する。そして、コンテンツ情報の受信が中断したときに鍵情報の変更を検出した場合は、初めてコンテンツ情報の受信側通信装置への送信を中断して、受信側通信装置が新しい鍵情報を取得するべく鍵情報の取得コマンドを送信することを促すものである。

これにより、従来装置のように、ノイズ等の送信の一時停止により、受信側通信装置が無駄に鍵情報の取得コマンドを送信して認証処理を行うということがなくなるため、結果的に通信速度が向上したネットワーク中継装置と通信装置、及びネットワーク中継方法を提供することができる。

【 0 0 0 9 】

【発明の実施の形態】

以下、図面を参照してこの発明の実施形態であるネットワーク中継装置及びネットワーク上の通信装置（通信機能をもったデジタル機器）の一例について、以下に詳細に説明する。

＜ネットワーク中継装置及び通信装置の構成＞

初めに、本発明に係るネットワーク中継装置及びネットワーク上の通信装置の構成について図面を用いて説明する。図 1 は、本発明に係るネットワーク中継装置の構成の一例を示すブロック図、図 2 は、本発明に係るネットワーク中継装置を用いたネットワークシステムを示すシステム図である。

【 0 0 1 0 】

本発明に係るネットワーク中継装置 1 0 は、図 2 に示すように、少なくとも 2 台、又はそれ以上を組として、両者で例えば無線通信を行い無線ネットワークを構築することで、例えば、USB (Universal Serial Bus) や、IEEE (Institute of Electrical and Electronics Engineers) 1 3 9 4 等による複数の第 1 のネットワーク N、N を中継する装置である。このようなネットワーク中継装置 1 0 の一例は、図 1 において、第 1 のネットワーク N に接続される第 1 のインタフェース 1 1 と、第 2 のネットワーク M に接続される第 2 のインタフェース 1 2 を有し、かつ、第 1 のネットワーク N と第 2 のネットワーク M とを接続する機能を有するネットワーク中継装置 1 0 において、第 1 のインタフェース 1 3 を介して受信しているコンテンツの暗号鍵番号をコンテンツの送信側通信装置 2 1 に問い合わせる鍵番号問合せ部 1 7 と、この鍵番号問合せ部 1 7 により取得した鍵番号が変更されたことを判定する鍵番号変更判定部 1 5 と、鍵番号変更判定部 1 5 により暗号鍵が変更された場合にそのことを第 2 のインタフェースを介して接続している受信側通信装置に通知する鍵番号変更通知部 1 6 とを有している。更

に、第 1 のインタフェース部 1 1 及び第 2 のインタフェース部 1 2 を介して送受信されるコンテンツ情報を一時的に格納しておくバッファ 1 8 と、全体の動作を制御する制御部 1 9 とを少なくとも有している。

このような本発明に係るネットワーク中継装置 1 0 は、図 2 に示すように、例えば、IEEE 1394 ネットワーク N 上に設けられた送信側通信装置 2 1 からコンテンツ情報を受信している。このコンテンツ情報は、例えば、D T C P (Digital Transmission Content Protection) により暗号化されている。コンテンツの送信側通信装置 2 1 は、コンテンツの受信側通信装置 2 2 と秘密の暗号鍵 $K \times 1$ を共有している。受信側通信装置 2 2 は、共有した秘密の鍵 $K \times 1$ により、暗号化されて伝送されたコンテンツ情報を復号化して受信する。

【 0 0 1 1 】

ここで、送信側通信装置 2 1 や受信側通信装置 2 2 は、例えば、通信機能を有した D T V (Digital Television) や D V R (Digital Video Recorder) 等のデジタル機器であってもよいし、通信機能をもった P C (Personal Computer) であってもよい。従って、送信処理を行う場合は送信側通信装置、受信処理を行う場合は受信側通信装置と呼んでいるが、通信機能をもったデジタル機器としての通信装置を意味するものである。

これらの通信装置 2 1, 2 2 は、少なくとも、ネットワーク N の通信規格（例えば、IEEE 1394）上の通信のためのインタフェースやバッファを内蔵する通信部 2 3 と、この通信部の通信動作を制御する制御部 2 4 とを有しており、ネットワーク N の通信規格に応じて、コンテンツ情報やコマンド等について、他のネットワーク上の通信機能をもった同様の通信装置同士と通信処理を行ない、更に、この通信規格に応じて、本発明に係るネットワーク中継装置 1 0 とも通信処理を行うものである。

送信側のネットワーク中継装置 1 0 は、例えば、D T C P 規格上の暗号化されたコンテンツ情報を復号化せずに無線ネットワークの受信側のネットワーク中継装置 1 0 に伝送する。暗号化されたコンテンツを受信した受信側のネットワーク中継装置 1 0 は、コンテンツを復号化せずにそのまま、例えば、IEEE 1394 ネットワーク N に伝送する。IEEE 1394 ネットワーク N 上に設けられた

受信側通信装置 2 2 は、コンテンツ情報を受信すると、予めコンテンツの送信側通信装置と認証をして得た暗号鍵を用いてコンテンツ情報を復号化して出力する。

【 0 0 1 2 】

<通信速度の遅延>

このようなネットワークを構築した本発明に係るネットワーク中継装置 1 0 においては、以下のように、ノイズ等による通信速度の遅延が発生する。図 3 乃至図 5 は、本発明に係るネットワーク中継装置の鍵番号変更通知を行わない際、送信側通信装置がコンテンツ送信を停止し再開した場合の通信動作を説明するフローチャートである。

【 0 0 1 3 】

すなわち、図 3 において、D T C P 規格において、送信側通信装置は、受信側通信装置と、コンテンツ情報の通信をしている (S 1 1) 。ここで、送信側通信装置は、ノイズ等の原因で又は本当に鍵変更のためにコンテンツの送信を停止する (S 1 2) 。その後、通信が再開した場合 (S 1 3) 、再開前の暗号鍵と異なる暗号鍵で暗号化してコンテンツを送る可能性がある。受信側通信装置は、コンテンツ伝送の停止を検知できるが、送信の停止前と再開後の暗号鍵の同一性について厳密に正確な判定はできないので、送信が停止するたびに、コンテンツを送信する毎に変わる鍵の番号を、A K E コマンドを送信側通信装置に送信することで確認する必要がでてくる (S 1 4) 。このため、通信が停止し再開するたびに鍵番号確認処理を行うことによって、通信の遅延が発生してしまう。

【 0 0 1 4 】

又、図 4 に示すように、本発明に係るネットワーク中継装置 1 0 を 2 台以上用いて、異なるネットワークの間の通信装置 2 1 , 2 2 同士でコンテンツ情報の D T C P 処理を伴う通信処理が行われている (S 2 1) 。このとき、ノイズ等が原因により、送信側通信装置 2 1 から送信側中継装置 1 0 へのコンテンツ情報の送信が中断された場合は、送信側中継装置 1 0 から受信側中継装置 1 0 ' へのコンテンツ情報の送信も中断され、受信側中継装置 1 0 ' から受信側通信装置 2 2 への送信も中断される (S 2 2) 。

【 0 0 1 5 】

その後、送信側通信装置 2 1 から送信側中継装置 1 0 へのコンテンツ情報が再開し、送信側中継装置 1 0 から受信側中継装置 1 0' への送信も、受信側中継装置 1 0' から受信側通信装置 2 2 への送信も再開する (S 2 3) 。このとき、注目すべきは、ノイズ等が原因で通信が中断したにもかかわらず、受信側通信装置 2 2 は、鍵番号が変更されたことにより中断した可能性があるため、鍵番号を A K E コマンドを送信側通信装置に送信することで確認することとなり (S 2 4) 、これが通信速度を低下させる原因となっている。

【 0 0 1 6 】

このような無駄な鍵認証処理を回避する手法としては、図 5 に示すように、受信側中継装置 1 0' において、空データ (空パケット) を受信側通信装置 2 2 に送信することで、受信側通信装置 2 2 の鍵認証処理を回避することができる。これにより、コンテンツ情報の送信が中断しても、鍵認証が起こることはなくなる。

【 0 0 1 7 】

しかしながら、図 5 に示すように、受信側通信装置 2 2 において、コンテンツ情報の中断が、ノイズ等の原因によるものか、本当に鍵番号の変更によるもののかを判断する働きがない場合は、正しい暗号鍵に変更する機会を得ることができない。すなわち、通常の無線伝送を行っている時 (S 3 1) 、鍵番号変更によりコンテンツ情報が中断すると (S 3 2) 、送信側中継装置 1 0 から受信側中継装置 1 0' への送信も中断するが、受信側中継装置 1 0' において、一律に空データを受信側通信装置 2 2 に送信すると (S 3 3) 、鍵認証処理が行われることがない。従って、ノイズ等が原因ではなくて、本当に鍵変更が行われた場合も、空データが受信側通信装置 2 2 に送信されることとなる。このため、受信側通信装置 2 2 は、コンテンツの暗号鍵が変更したことを知ることができないため、正しい暗号鍵を得ることができず、コンテンツ情報の復号化に失敗して、例えば、正しい映像情報を得ることができないこととなる (S 3 4) 。

【 0 0 1 8 】

< 第 1 の鍵変更通知方法 >

本発明に係るネットワーク中継装置 1 0 においては、送信側中継装置 1 0 において、少なくとも、図 1 に示した鍵番号問い合わせ部 1 7 と、鍵番号変更判定部 1 5 と、鍵番号変更通知部 1 6 との働きにより、鍵番号変更を検出すると、受信側中継装置 1 0 に鍵変更通知信号を送信する。更に、受信側のネットワーク中継装置 1 0' では、コンテンツ情報の中断があり鍵変更通知信号を受けない時は、空データを受信側通信装置 2 2 に送信することにより、無駄な鍵認証処理を回避することで、通信速度の低下を回避し、コンテンツ情報の中断があり鍵変更通知信号を伴う場合は、空データも送らず、コンテンツ情報の送信を中断することで、受信側通信装置 2 2 に鍵認証処理を促し、新しい鍵情報の取得をさせるものである。

【 0 0 1 9 】

すなわち、図 6 において、本発明に係るネットワーク中継装置 1 0, 1 0' を用いて、送信側通信装置 2 1 と受信側通信装置 2 2 との通信を行っている際に (S 4 1)、コンテンツ情報の送信が中断すると、送信側中継装置 1 0 からの送信も中断し、受信側中継装置 1 0' においては、鍵変更通知信号が送信されていないことを確認して、空データを受信側通信装置 2 2 へと送信する (S 4 2)。これにより、受信側通信装置 2 2 において、無駄な鍵認証処理が行われることで通信速度が低下することがない。

【 0 0 2 0 】

更に、送信側通信装置 2 1 において、鍵番号 A K 1 が鍵番号 A K 2 に変更となって通信が再開されると (S 4 3)、送信側中継装置 1 0 においては、鍵番号問い合わせ部 1 7 から A K E コマンドである問合せ信号を送信側通信装置 2 1 に送信し、これに応じて送信側通信装置 2 1 から出力された鍵番号信号を受けて、鍵番号変更判定部 1 5 において、鍵番号が変更されたか否かを判断する。そして、鍵番号が変更されたと判断されたことが鍵番号変更通知部 1 6 に伝わると、鍵番号変更通知部 1 6 は、鍵変更通知信号を生成して、第 2 のインタフェース部 1 2 を介して、無線ネットワーク M を介して、受信側中継装置 1 0' に鍵変更通知信号を送信する (S 4 4)。

【 0 0 2 1 】

尚、ここで、AKEコマンドである問合せ信号を送信側通信装置21に送信するタイミングは、コンテンツ情報が中断して再開した時点としたが、これに限定されるものではなく、コンテンツ情報が一定期間中断した時点であることも可能であり、又、他のタイミングで行うことも可能である。

【0022】

受信側中継装置10'では、この鍵変更通知信号を受けると、空データの受信側通信装置22への送信を一時中断し(S45)、受信側通信装置22が新たな鍵番号を取得するべくAKEコマンドである問合せ信号を送信側通信装置21へ送信することを促す。これにより、コンテンツ情報(又は空データ)等の送信信号が一定期間中断すると、現行のDTCF規格等による規定により、受信側通信装置22は、新たな鍵番号を取得する処理を行う(S46)。従って、受信側中継装置10'が送信を一時中断することにより、受信側通信装置22は、新しい鍵番号を取得することができるため、迅速な鍵番号取得による新たな鍵情報により、通信処理が再開されることとなる(S47)。

【0023】

これにより、本発明に係るネットワーク中継装置によれば、無駄な鍵番号の検出を行わないことで速度低下を回避しながら、必要な鍵変更時の鍵番号の検出を確実に行うことにより、確実に迅速な通信処理を行うことが可能となる。

<第2の鍵変更通知方法>

第1の鍵変更通知方法においては、本発明に係るネットワーク中継装置10、10'の間だけの、鍵変更通知信号の生成とこれに応じるコンテンツ転送中断による処理によって、速度低下を回避していた。しかし、本発明はこれに限らず、送信側中継装置10で生成した鍵変更通知信号を直接、受信側通信装置22に転送して、受信側通信装置22にこれに応じて、新しい鍵番号の取得を促す方法を提示するものである。この方法によれば、受信側通信装置22において、鍵変更通知信号を認識する働きと、これに応じて新しい鍵番号の取得処理を設定しておくことで、受信側中継装置10'において、コンテンツ情報の転送を中断する必要がなくなるため、より高い転送速度を可能とする。図7は、本発明に係るネットワーク中継装置において、鍵番号変更通知を行うことにより、再認証を行う場

合の通信動作を説明するフローチャートである。

【 0 0 2 4 】

すなわち、本発明に係る第2の鍵変更通知方法による処理は、図7のフローチャートにおいて、本発明に係るネットワーク中継装置10、10'を用いて、送信側通信装置21と受信側通信装置22との通信を行っている際に(S51)、コンテンツ情報の送信が中断すると、送信側中継装置10からの送信も中断し、受信側中継装置10'においては、鍵変更通知信号が送信されていないことを確認して、空データを受信側通信装置22へと送信する(S52)。これにより、受信側通信装置22において、無駄な鍵認証処理による通信速度の低下が回避される。

更に、送信側通信装置21において、鍵番号AK1が鍵番号AK2に変更となって通信が再開されると(S53)、送信側中継装置10においては、鍵番号問い合わせ部17からAKEコマンドである問合せ信号を送信側通信装置21に送信し、これに応じて送信側通信装置21から出力された鍵番号信号を受けて、鍵番号変更判定部15において、鍵番号が変更されたか否かを判断する。そして、鍵番号が変更されたと判断されたことが鍵番号変更通知部16に伝わると、鍵番号変更通知部16は、鍵変更通知信号を生成して、第2のインタフェース部12を介して、無線ネットワークM及び中継相手である受信側中継装置10'を介して、受信側通信装置22に鍵変更通知信号を送信する(S54)。

【 0 0 2 5 】

尚、第1の鍵変更通知方法と同様に、AKEコマンドである問合せ信号を送信側通信装置21に送信するタイミングは、コンテンツ情報が中断して再開した時点としたが、これに限定されるものではなく、コンテンツ情報が一定期間中断した時点であることも可能であり、又、他のタイミングで行うことも可能である。

【 0 0 2 6 】

受信側通信装置22では、鍵変更通知信号を受けて、図1で示した通信部23と制御部24との働きにより、新たな鍵番号を取得するべくAKEコマンドである問合せ信号を送信側通信装置21へ送信する(S55)。これに応じて送信側通信装置21から送信された鍵情報を取得し、受信側通信装置22では、新たな

鍵情報により、受信したコンテンツ情報の復号処理を行う。

従って、本発明に係る第 2 の鍵変更通知方法によれば、ノイズ等によるコンテンツ情報の送信が中断しても、又は、鍵番号の変更による送信中断があっても、送信側通信装置 2 1 と受信側通信装置 2 2 との送信処理が中断されることなく、従来装置に比べて、確実に高速な通信処理を行うことが可能となる。

又、更に、本発明は、上述したように、二つのネットワークを一つの無線ネットワークで中継する場合だけではなく、図 8 に示すように、送信側中継装置 2 3 と受信側通信装置 2 4 との間を一つの無線ネットワーク M と一つのネットワーク N とを介して送受信する場合にも適用することができる。

なお、上述した実施形態は、通信規格を I E E E 1 3 9 4 や U S B の場合について、暗号方法を D T C P の場合について説明したが、通信規格や暗号方法はこれに限らない。

【 0 0 2 7 】

以上記載した様々な実施形態により、当業者は本発明を実現することができるが、更にこれらの実施形態の様々な変形例を思いつくことが当業者によって容易であり、発明的な能力をもたなくとも様々な実施形態へと適用することが可能である。従って、本発明は、開示された原理と新規な特徴に矛盾しない広範な範囲に及ぶものであり、上述した実施形態に限定されるものではない。

【 0 0 2 8 】

【発明の効果】

以上、詳述したように本発明によれば、コンテンツの鍵番号が変更されたことを即座に受信側のネットワーク中継装置に通知することにより、即座に鍵検出を行うことができ、更にノイズ等による送信中断があっても鍵変更がなければ空データを送信することにより、無駄な認証や鍵検出を行うことがないため、従来装置にくらべて処理速度を向上させることが可能なネットワーク中継装置を提供することができる。

【図面の簡単な説明】

【図 1】

本発明に係るネットワーク中継装置の構成の一例を示すブロック図。

【図 2】

本発明に係るネットワーク中継装置を用いたネットワークシステムを示すシステム図。

【図 3】

本発明に係るネットワーク中継装置の鍵番号変更通知を行わない際、送信側通信装置がコンテンツ送信を停止し再開した場合の通信動作を説明するフローチャート。

【図 4】

本発明に係るネットワーク中継装置の鍵番号変更通知を行わない際、送信側通信装置がコンテンツ送信を停止し再開した場合の通信動作を説明するフローチャート。

【図 5】

本発明に係るネットワーク中継装置の鍵番号変更通知を行わない際、送信側通信装置がコンテンツ送信を停止し再開した場合の通信動作を説明するフローチャート。

【図 6】

本発明に係るネットワーク中継装置において、鍵番号変更通知を行うことにより、再認証を行う場合の通信動作を説明するフローチャート。

【図 7】

本発明に係るネットワーク中継装置において、鍵番号変更通知を行うことにより、再認証を行う場合の通信動作を説明するフローチャート。

【図 8】

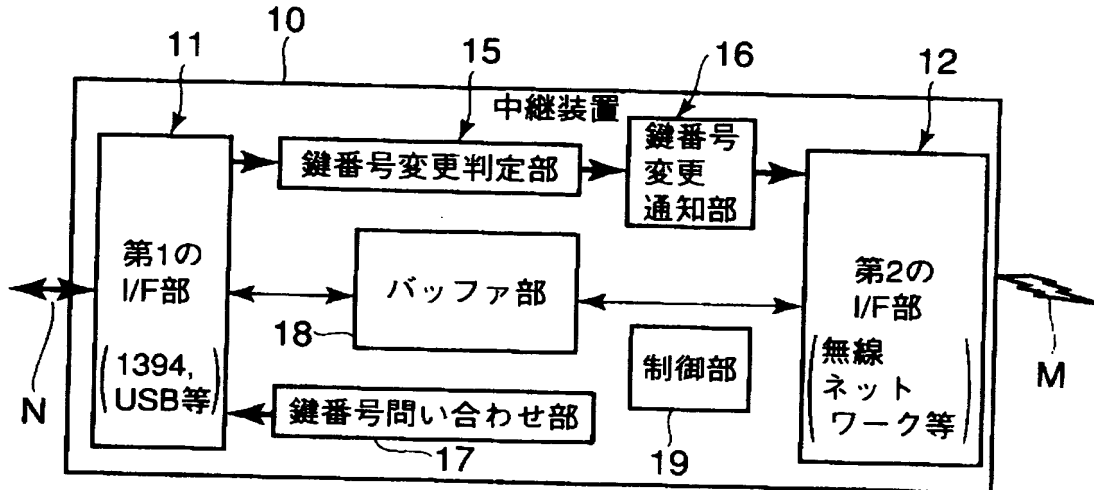
本発明に係るネットワーク中継装置を用いた他のネットワークシステムを示すシステム図。

【符号の説明】

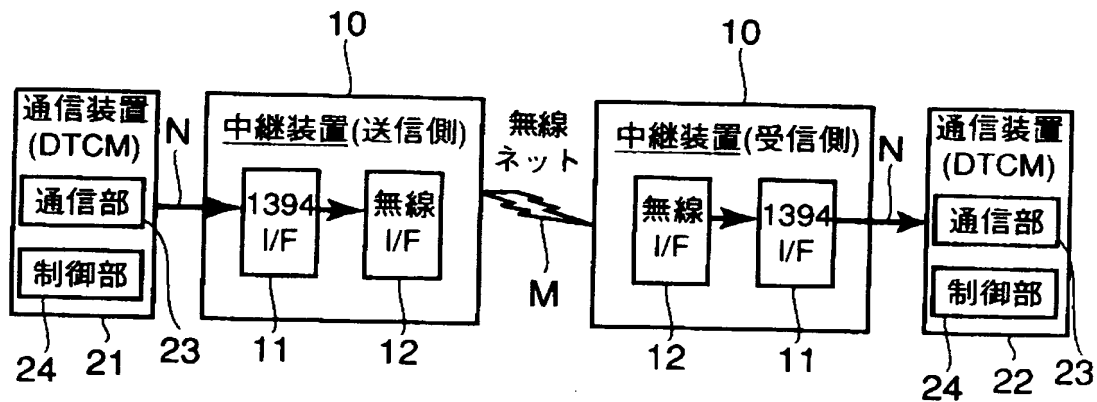
1 0 … ネットワーク中継装置、 1 1 … 第 1 のインタフェース部、 1 2 … 第 2 のインタフェース部、 1 3 … 制御部、 1 5 … 鍵番号変更判定部、 1 6 … 鍵番号変更通知部、 1 7 … 鍵番号問い合わせ部、 1 8 … バッファ部、 1 9 … 制御部。

【書類名】 図面

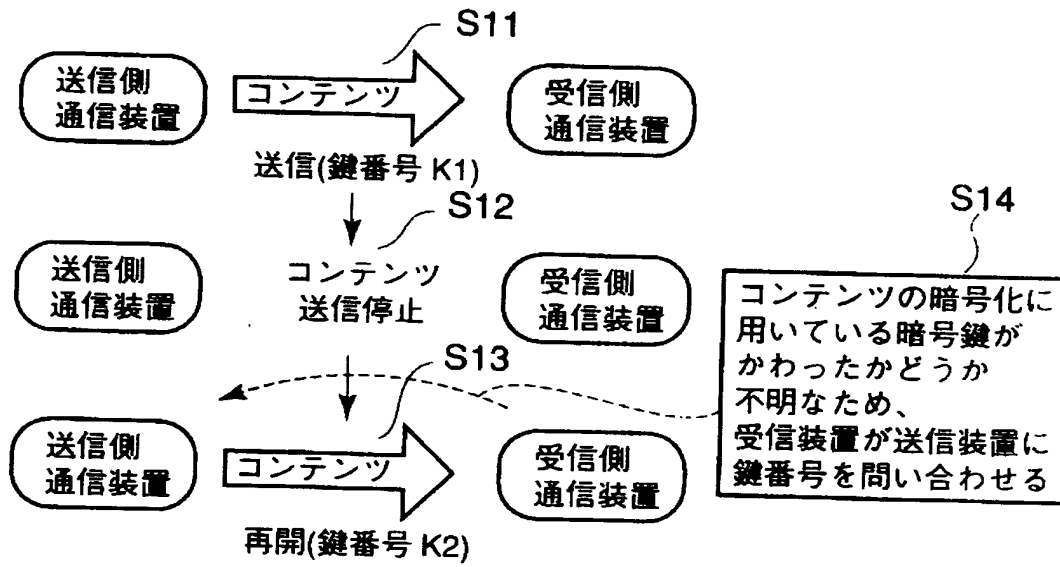
【図 1】



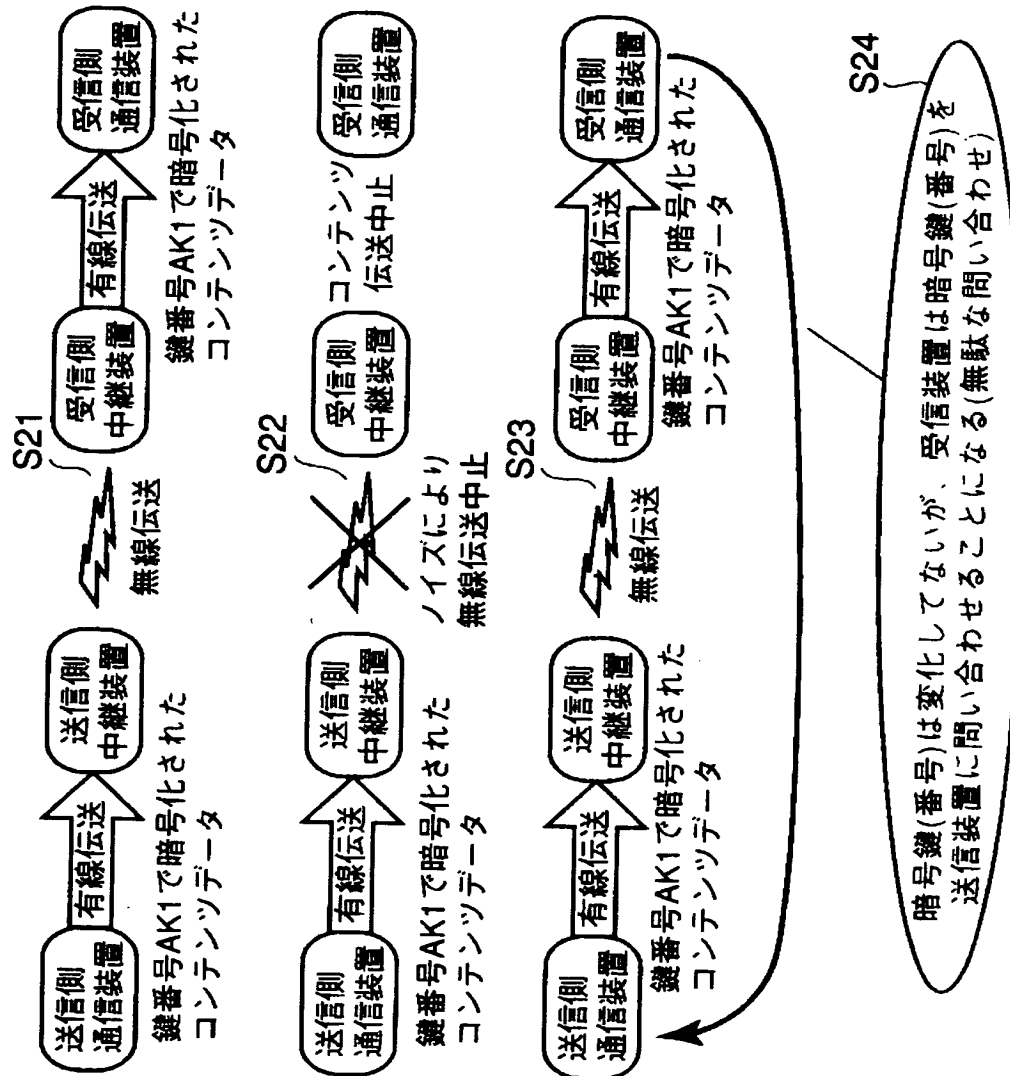
【図 2】



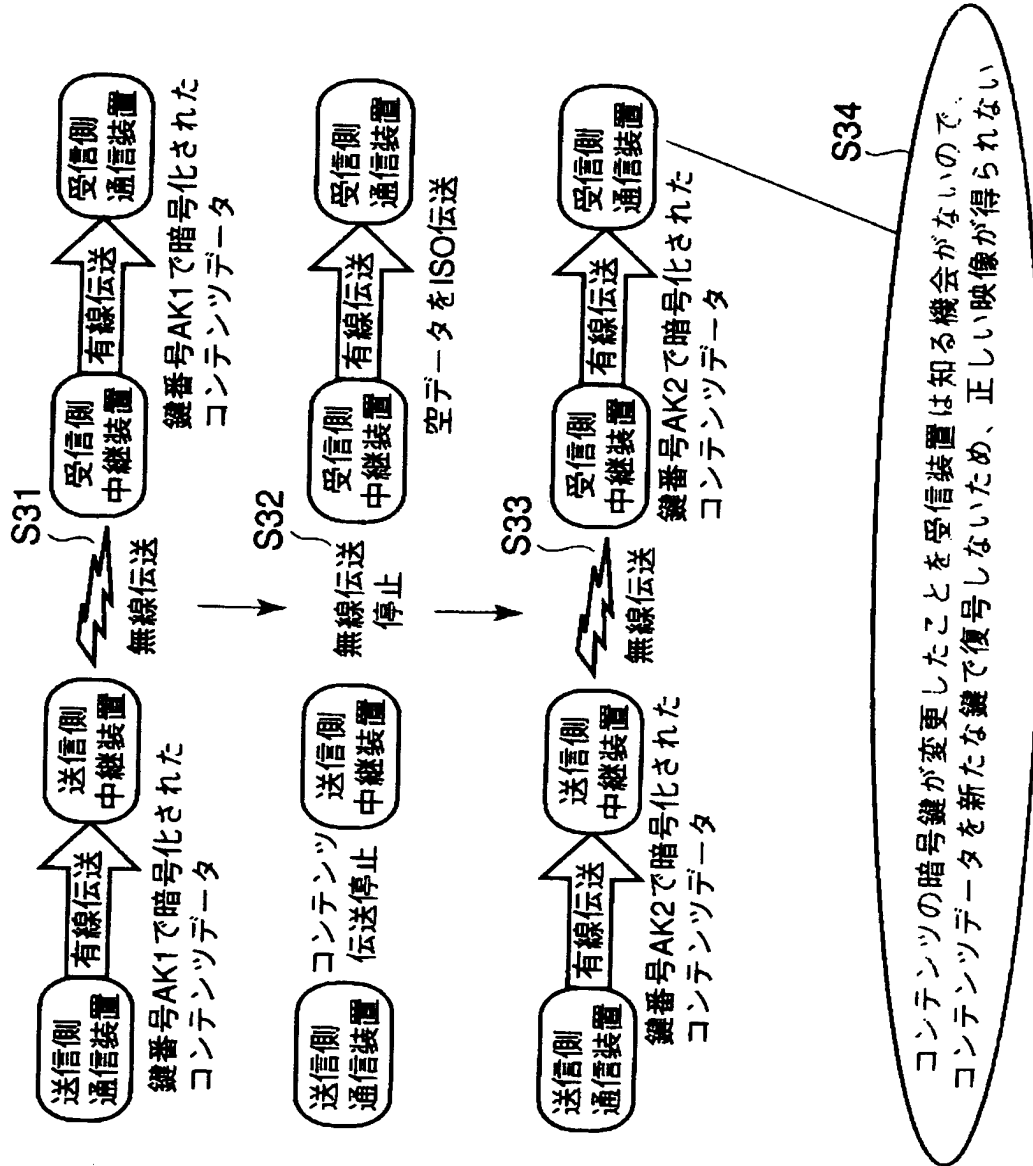
【図 3】



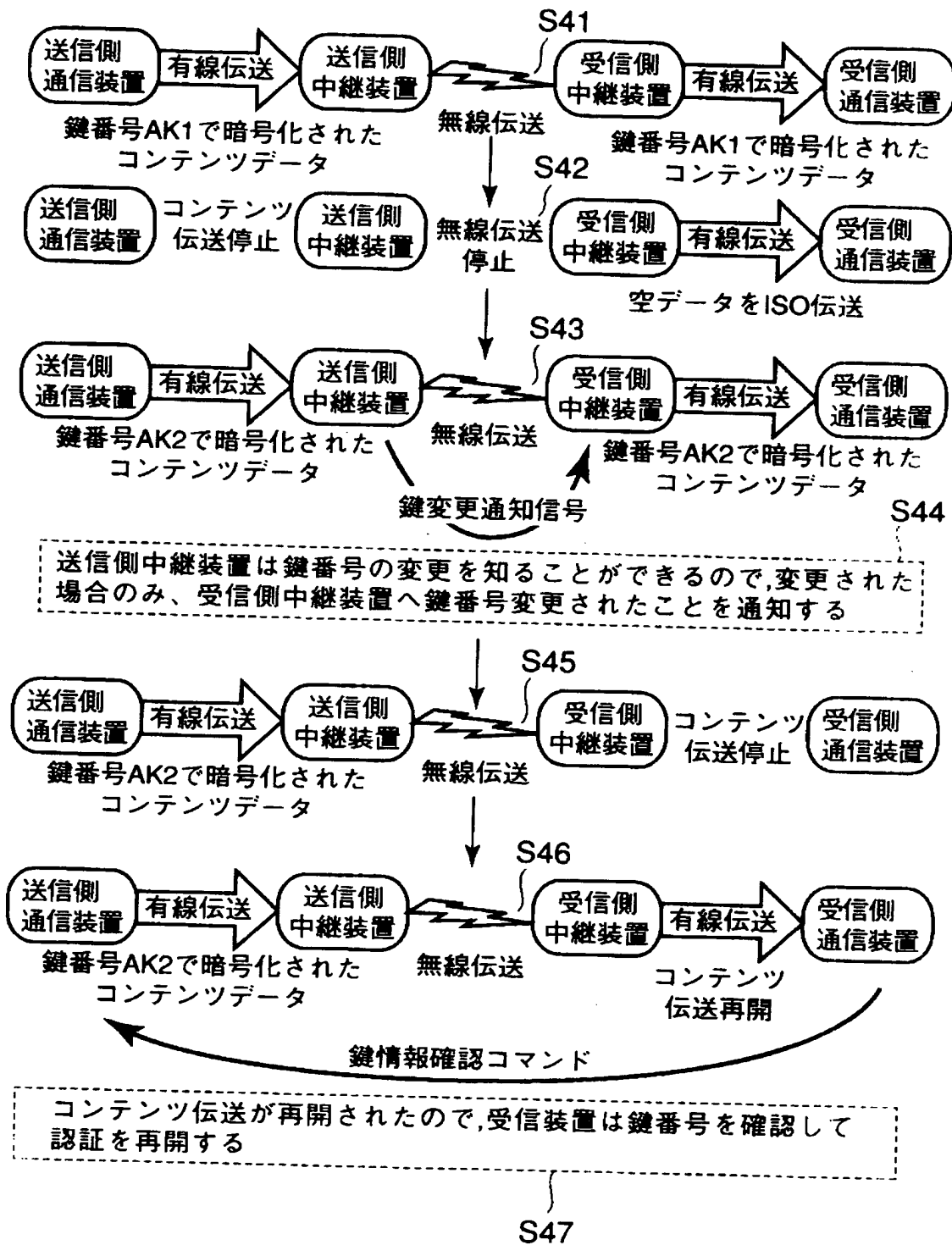
【図 4】



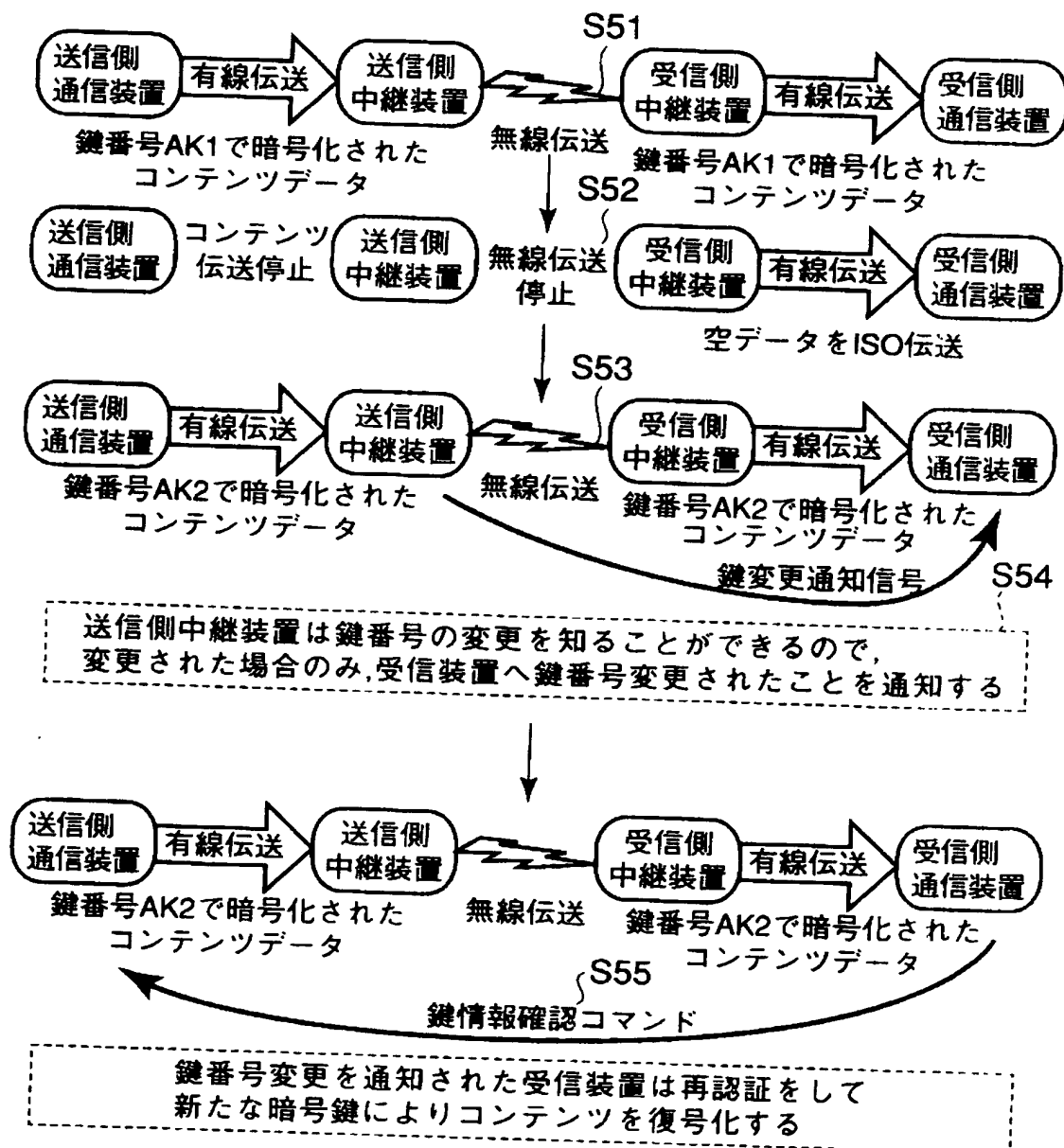
【図 5】



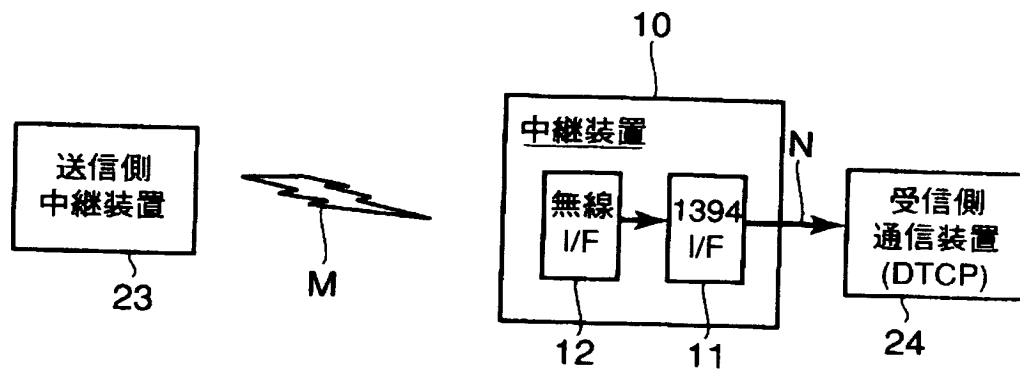
【図6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 ネットワーク上の暗号鍵の変更を検出し、鍵変更通知信号として受信側中継装置に送信することで、高速化されたネットワーク中継装置を提供する。

【解決手段】 第1ネットワークNに接続され鍵情報により暗号化されたコンテンツ情報を送信する第1インタフェース11と、第2ネットワークMに接続され受信側ネットワーク中継装置へコンテンツ情報を送信する第2インタフェース12と、この鍵情報の変更を検出して鍵変更通知信号を受信側ネットワーク中継装置に通知する通知部15、16、17とをもつネットワーク中継装置。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝